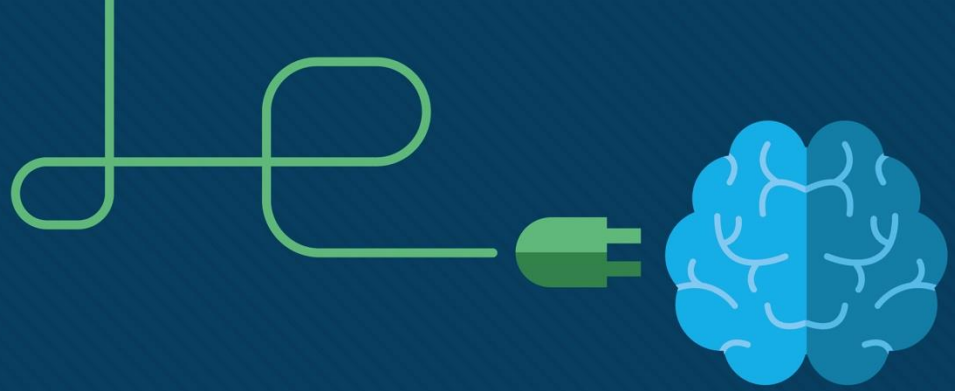


Module 12: WLAN Concepts

Instructor Materials

Switching, Routing and Wireless Essentials v7.0 (SRWE)

12.1 Introduction to Wireless

802.11 Standards

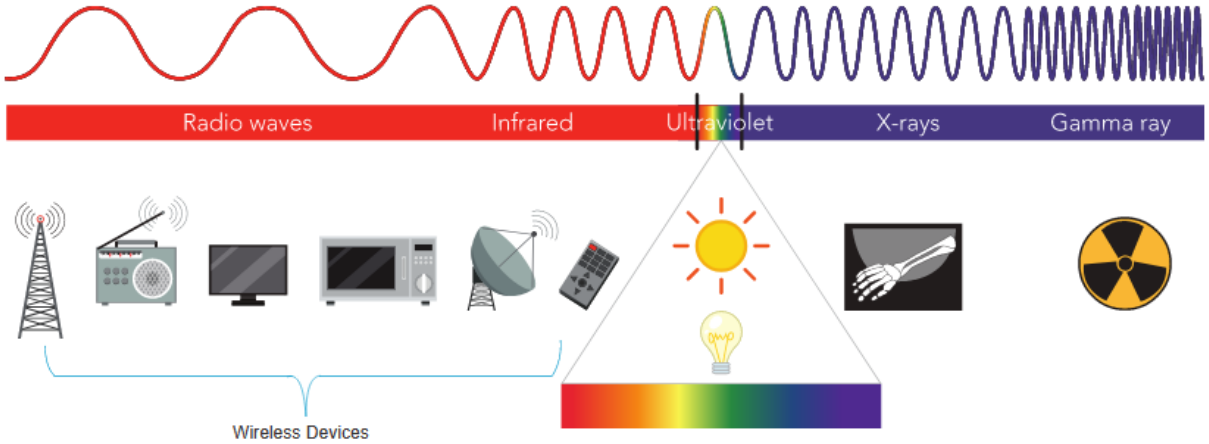
802.11 WLAN standards define how radio frequencies are used for wireless links.

IEEE Standard	Radio Frequency	Description
802.11	2.4 GHz	Data rates up to 2 Mb/s
802.11a	5 GHz	Data rates up to 54 Mb/s Not interoperable with 802.11b or 802.11g
802.11b	2.4 GHz	Data rates up to 11 Mb/s Longer range than 802.11a and better able to penetrate building structures
802.11g	2.4 GHz	Data rates up to 54 Mb/s Backward compatible with 802.11b
802.11n	2.4 and 5 GHz	Data rates 150 – 600 Mb/s Require multiple antennas with MIMO technology
802.11ac	5 GHz	Data rates 450 Mb/s – 1.3 Gb/s Supports up to eight antennas
802.11ax	2.4 and 5 GHz	High-Efficiency Wireless (HEW) Capable of using 1 GHz and 7 GHz frequencies

Radio Frequencies

All wireless devices operate in the range of the electromagnetic spectrum. WLAN networks operate in the 2.4 and 5 GHz frequency bands.

- 2.4 GHz (UHF) – 802.11b/g/n/ax
- 5 GHz (SHF) – 802.11a/n/ac/ax



12.2 WLAN Components

Wireless NICs

To communicate wirelessly, laptops, tablets, smart phones, and even the latest automobiles include integrated wireless NICs that incorporate a radio transmitter/receiver.

If a device does not have an integrated wireless NIC, then a USB wireless adapter can be used.

Wireless Home Router

A home user typically interconnects wireless devices using a small, wireless router.

Wireless routers serve as the following:

- **Access point** – To provide wires access
- **Switch** – To interconnect wired devices
- **Router** - To provide a default gateway to other networks and the Internet

Wireless Access Point

Wireless clients use their wireless NIC to discover nearby access points (APs).

Clients then attempt to associate and authenticate with an AP.

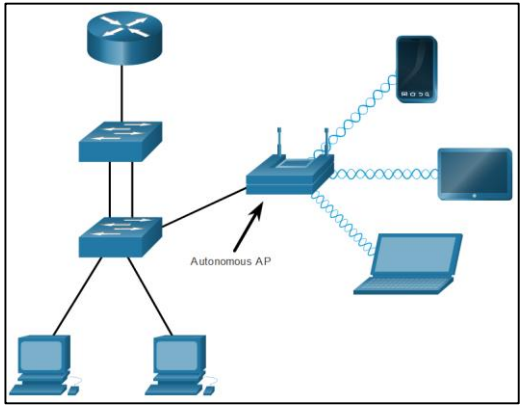
After being authenticated, wireless users have access to network resources.

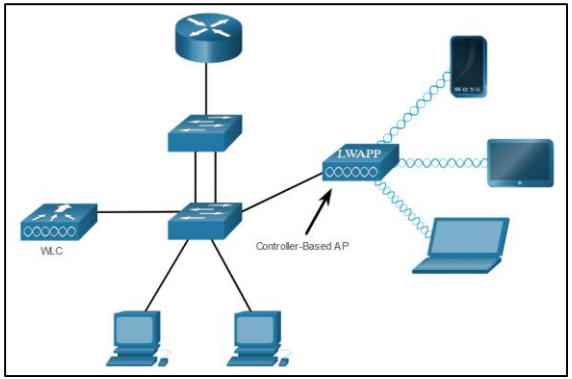
Cisco Meraki Go access points

AP Categories

APs can be categorized as either autonomous APs or controller-based APs.

- **Autonomous APs** – Standalone devices configured through a command line interface or GUI. Each autonomous AP acts independently of the others and is configured and managed manually by an administrator.
- **Controller-based APs** – Also known as lightweight APs (LAPs). Use Lightweight Access Point Protocol (LWAPP) to communicate with a LWAN controller (WLC). Each LAP is automatically configured and managed by the WLC.





Wireless Antennas

Types of external antennas:

- **Omnidirectional** – Provide 360-degree coverage. Ideal in houses and office areas.
- **Directional** – Focus the radio signal in a specific direction. Examples are the Yagi and parabolic dish.
- **Multiple Input Multiple Output (MIMO)** – Uses multiple antennas (Up to eight) to increase bandwidth.

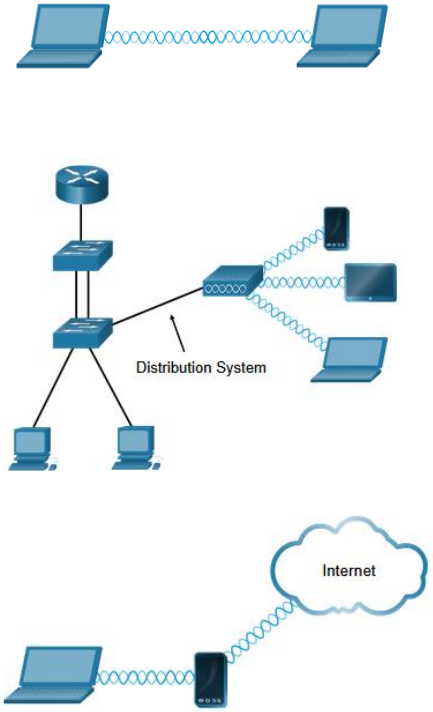
12.3 WLAN Operation

802.11 Wireless Topology Modes

Ad hoc mode - Used to connect clients in peer-to-peer manner without an AP.

Infrastructure mode - Used to connect clients to the network using an AP.

Tethering - Variation of the ad hoc topology is when a smart phone or tablet with cellular data access is enabled to create a personal hotspot.



BSS and ESS

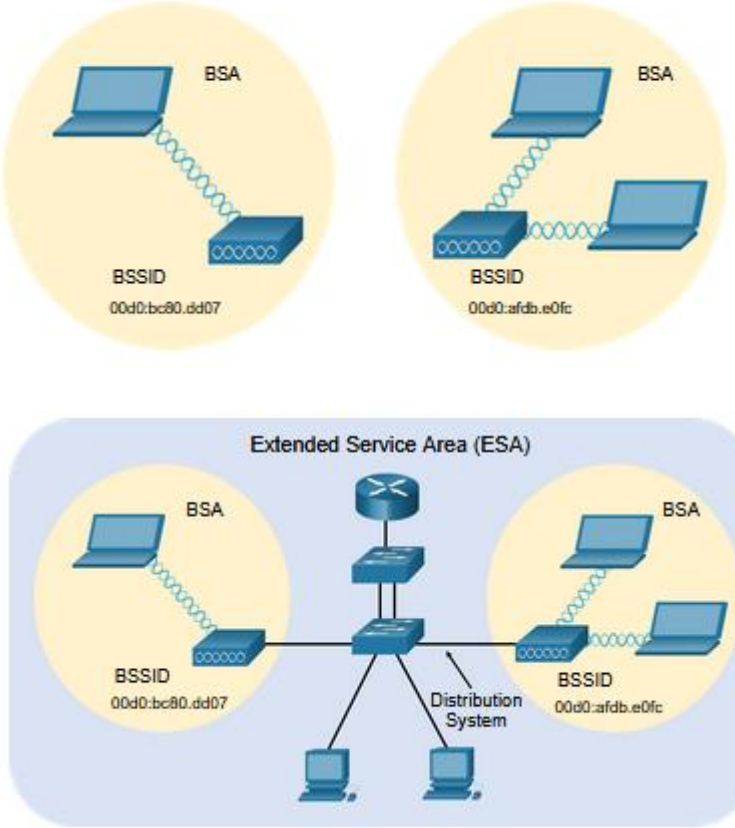
Infrastructure mode defines two topology blocks:

Basic Service Set (BSS)

- Uses single AP to interconnect all associated wireless clients.
- Clients in different BSSs cannot communicate.

Extended Service Set (ESS)

- A union of two or more BSSs interconnected by a wired distribution system.
- Clients in each BSS can communication through the ESS.



CSMA/CA

WLANs are half-duplex and a client cannot “hear” while it is sending, making it impossible to detect a collision.

WLANs use carrier sense multiple access with collision avoidance (CSMA/CA) to determine how and when to send data. A wireless client does the following:

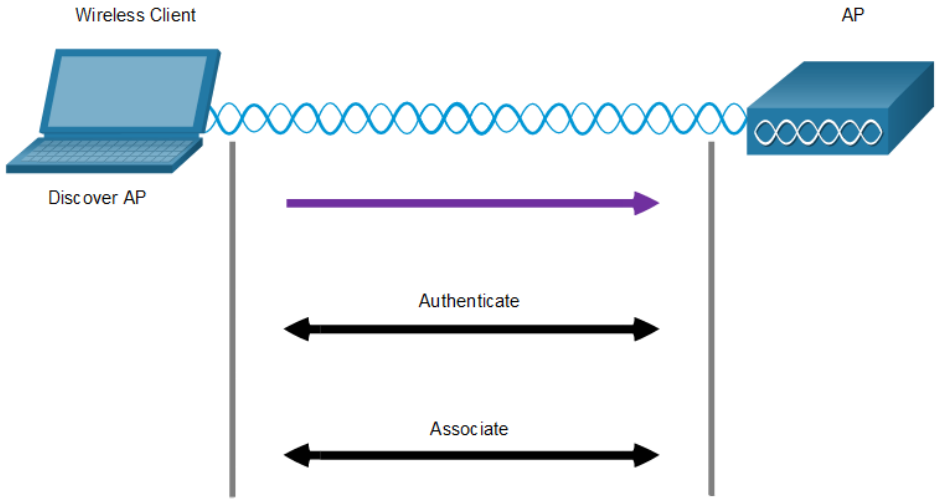
1. Listens to the channel to see if it is idle, i.e. no other traffic currently on the channel.
2. Sends a ready to send (RTS) message the AP to request dedicated access to the network.
3. Receives a clear to send (CTS) message from the AP granting access to send.
4. Waits a random amount of time before restarting the process if no CTS message received.
5. Transmits the data.
6. Acknowledges all transmissions. If a wireless client does not receive an acknowledgment, it assumes a collision occurred and restarts the process

Wireless Client and AP Association

For wireless devices to communicate over a network, they must first associate with an AP or wireless router.

Wireless devices complete the following three stage process:

- Discover a wireless AP
- Authenticate with the AP
- Associate with the AP



Wireless Client and AP Association (Cont.)

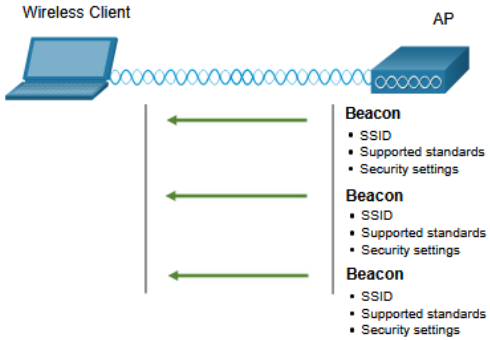
To achieve successful association, a wireless client and an AP must agree on specific parameters:

- **SSID** – The client needs to know the name of the network to connect.
- **Password** – This is required for the client to authenticate to the AP.
- **Network mode** – The 802.11 standard in use.
- **Security mode** – The security parameter settings, i.e. WEP, WPA, or WPA2.
- **Channel settings** – The frequency bands in use.

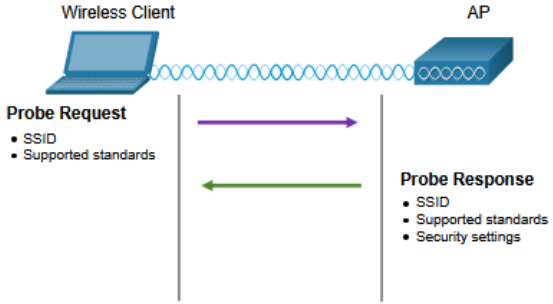
Passive and Active Discover Mode

Wireless clients connect to the AP using a passive or active scanning (probing) process.

- **Passive mode** – AP openly advertises its service by periodically sending broadcast beacon frames containing the SSID, supported standards, and security settings.
- **Active mode** – Wireless clients must know the name of the SSID. The wireless client initiates the process by broadcasting a probe request frame on multiple channels.



Passive mode

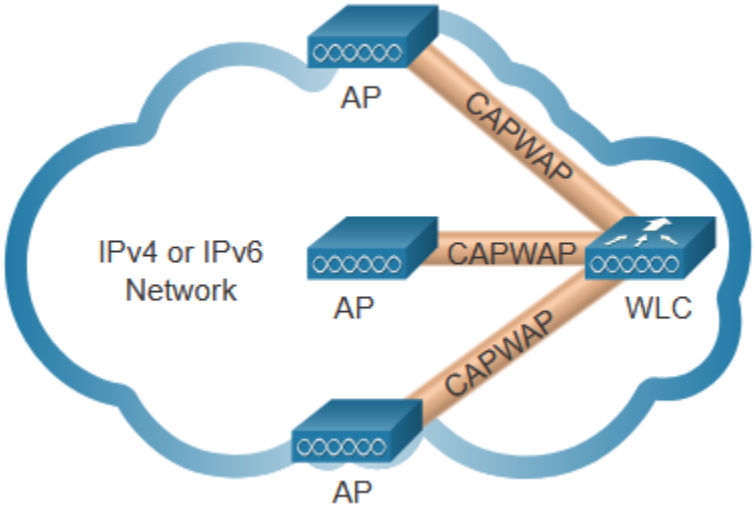


Active mode

12.4 CAPWAP Operation

Introduction to CAPWAP

- CAPWAP is an IEEE standard protocol that enables a WLC to manage multiple APs and WLANs.
- Based on LWAPP but adds additional security with Datagram Transport Layer Security (DLTS).
- Encapsulates and forwards WLAN client traffic between an AP and a WLC over tunnels using UDP ports 5246 and 5247.
- Operates over both IPv4 and IPv6. IPv4 uses IP protocol 17 and IPv6 uses IP protocol 136.



Split MAC Architecture

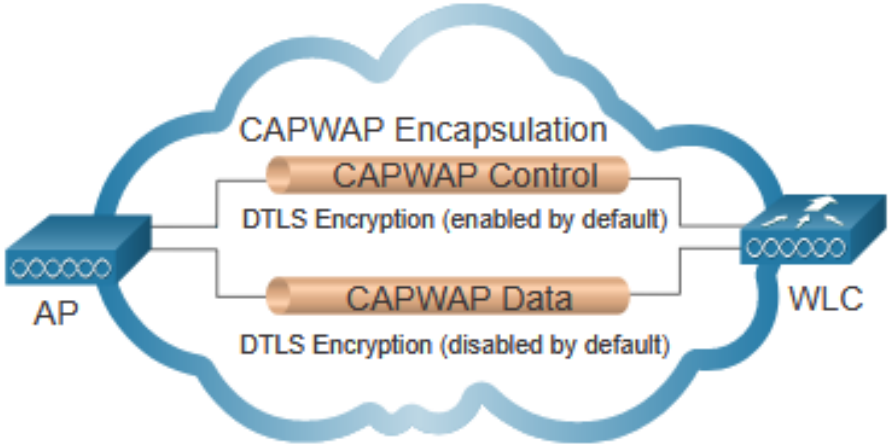
The CAPWAP split MAC concept does all the functions normally performed by individual APs and distributes them between two functional components:

- AP MAC Functions
- WLC MAC Functions

AP MAC Functions	WLC MAC Functions
Beacons and probe responses	Authentication
Packet acknowledgements and retransmissions	Association and re-association of roaming clients
Frame queueing and packet prioritization	Frame translation to other protocols
MAC layer data encryption and decryption	Termination of 802.11 traffic on a wired interface

DTLS Encryption

- DTLS provides security between the AP and the WLC.
- It is enabled by default to secure the CAPWAP control channel and encrypt all management and control traffic between AP and WLC.
- Data encryption is disabled by default and requires a DTLS license to be installed on the WLC before it can be enabled on the AP.

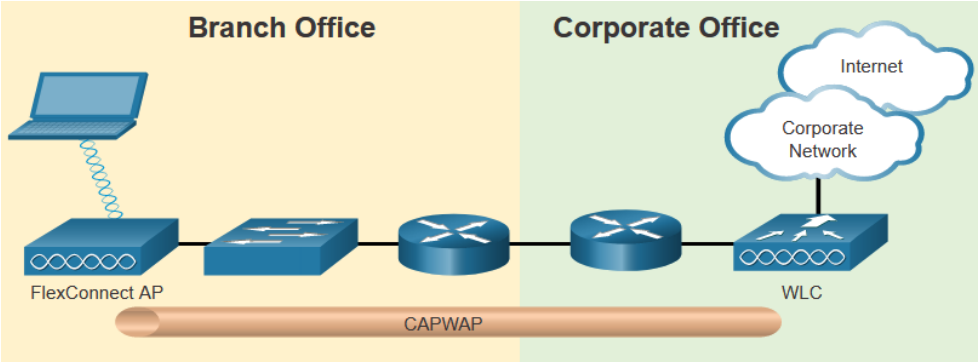


Flex Connect APs

FlexConnect enables the configuration and control of Aps over a WAN link.

There are two modes of option for the FlexConnect AP:

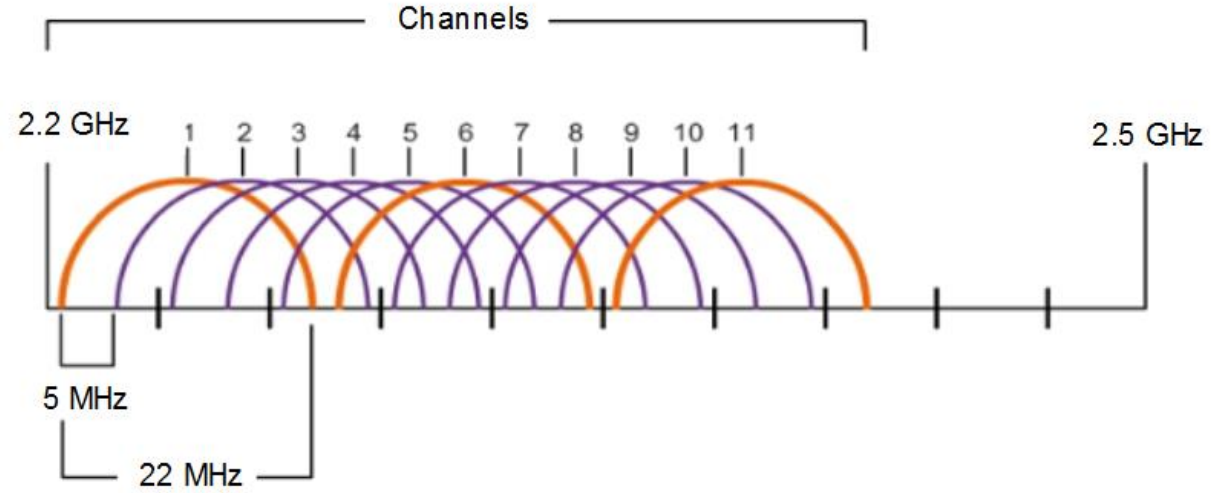
- **Connected mode** – The WLC is reachable. The FlexConnect AP has CAPWAP connectivity with the WLC through the CAPWAP tunnel. The WLC performs all CAPWAP functions.
- **Standalone mode** – The WLC is unreachable. The FlexConnect AP has lost CAPWAP connectivity with the WLC. The FlexConnect AP can assume some of the WLC functions such as switching client data traffic locally and performing client authentication locally.



12.5 Channel Management

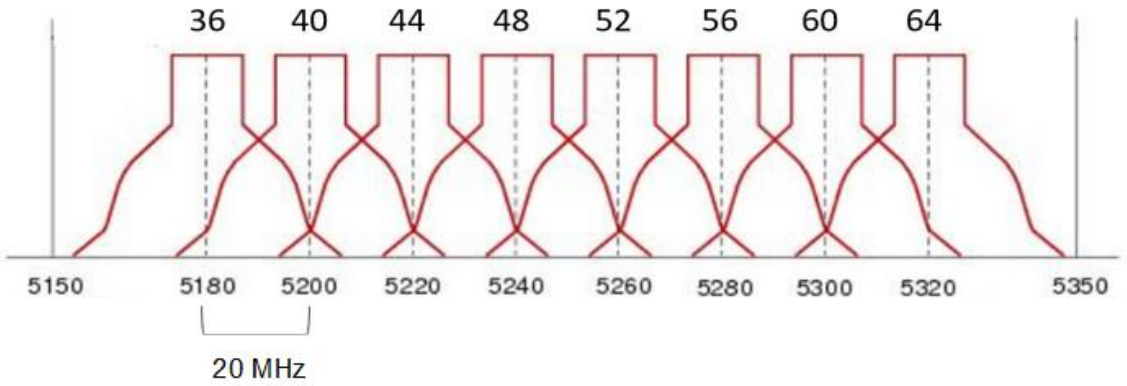
Channel Selection

- The 2.4 GHz band is subdivided into multiple channels each allotted 22 MHz bandwidth and separated from the next channel by 5 MHz.
- A best practice for 802.11b/g/n WLANs requiring multiple APs is to use non-overlapping channels such as 1, 6, and 11.



Channel Selection (Cont.)

- For the 5GHz standards 802.11a/n/ac, there are 24 channels. Each channel is separated from the next channel by 20 MHz.
- Non-overlapping channels are 36, 48, and 60.

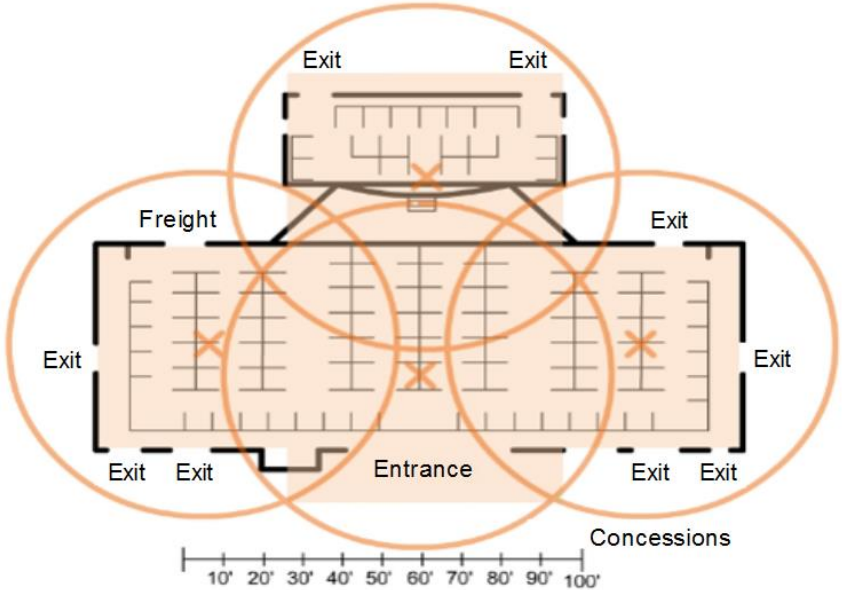


Plan a WLAN Deployment

The number of users supported by a WLAN depends on the following:

- The geographical layout of the facility
- The number of bodies and devices that can fit in a space
- The data rates users expect
- The use of non-overlapping channels by multiple APs and transmit power settings

When planning the location of APs, the approximate circular coverage area is important.



12.6 WLAN Threats

Wireless Security Overview

A WLAN is open to anyone within range of an AP and the appropriate credentials to associate to it.

Attacks can be generated by outsiders, disgruntled employees, and even unintentionally by employees. Wireless networks are specifically susceptible to several threats, including the following:

- Interception of data
- Wireless intruders
- Denial of Service (DoS) Attacks
- Rogue APs

DoS Attacks

Wireless DoS attacks can be the result of the following:

- Improperly configured devices
- A malicious user intentionally interfering with the wireless communication
- Accidental interference

To minimize the risk of a DoS attack due to improperly configured devices and malicious attacks, harden all devices, keep passwords secure, create backups, and ensure that all configuration changes are incorporated off-hours.

Rogue Access Points

- A rogue AP is an AP or wireless router that has been connected to a corporate network without explicit authorization and against corporate policy.
- Once connected, the rogue AP can be used by an attacker to capture MAC addresses, capture data packets, gain access to network resources, or launch a man-in-the-middle attack.
- A personal network hotspot could also be used as a rogue AP. For example, a user with secure network access enables their authorized Windows host to become a Wi-Fi AP.
- To prevent the installation of rogue APs, organizations must configure WLCs with rogue AP policies and use monitoring software to actively monitor the radio spectrum for unauthorized APs.

Man-in-the-Middle Attack

In a man-in-the-middle (MITM) attack, the hacker is positioned in between two legitimate entities in order to read or modify the data that passes between the two parties. A popular wireless MITM attack is called the “evil twin AP” attack, where an attacker introduces a rogue AP and configures it with the same SSID as a legitimate AP.

Defeating a MITM attack begins with identifying legitimate devices on the WLAN. To do this, users must be authenticated. After all of the legitimate devices are known, the network can be monitored for abnormal devices or traffic.

12.7 Secure WLANs

SSID Cloaking and MAC Address Filtering

To address the threats of keeping wireless intruders out and protecting data, two early security features were used and are still available on most routers and APs:

SSID Cloaking

- APs and some wireless routers allow the SSID beacon frame to be disabled. Wireless clients must be manually configured with the SSID to connect to the network.

MAC Address Filtering

- An administrator can manually permit or deny clients wireless access based on their physical MAC hardware address. In the figure, the router is configured to permit two MAC addresses. Devices with different MAC addresses will not be able to join the 2.4GHz WLAN.

802.11 Original Authentication Methods

The best way to secure a wireless network is to use authentication and encryption systems. Two types of authentication were introduced with the original 802.11 standard:

Open system authentication

- No password required. Typically used to provide free internet access in public areas like cafes, airports, and hotels.
- Client is responsible for providing security such as through a VPN.

Shared key authentication

- Provides mechanisms, such as WEP, WPA, WPA2, and WPA3 to authenticate and encrypt data between a wireless client and AP. However, the password must be pre-shared between both parties to connect.

Shared Key Authentication Methods

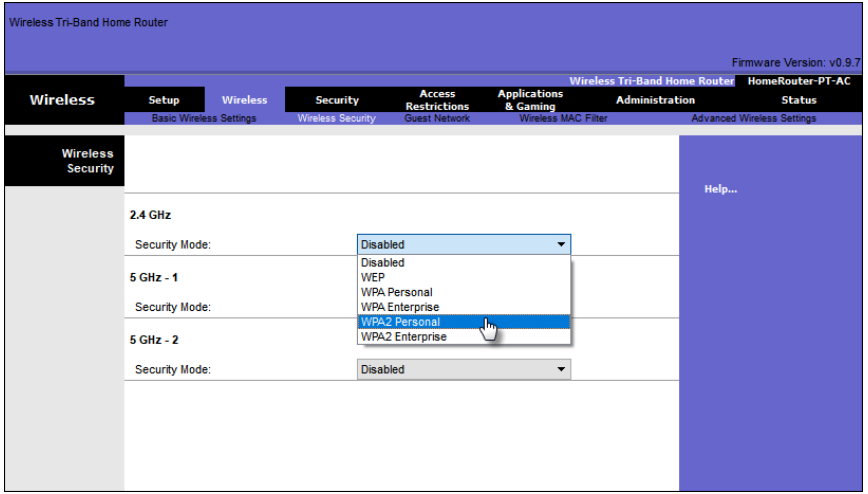
There are currently four shared key authentication techniques available, as shown in the table.

Authentication Method	Description
Wired Equivalent Privacy (WEP)	The original 802.11 specification designed to secure the data using the Rivest Cipher 4 (RC4) encryption method with a static key. WEP is no longer recommended and should never be used.
Wi-Fi Protected Access (WPA)	A Wi-Fi Alliance standard that uses WEP but secures the data with the much stronger Temporal Key Integrity Protocol (TKIP) encryption algorithm. TKIP changes the key for each packet, making it much more difficult to hack.
WPA2	It uses the Advanced Encryption Standard (AES) for encryption. AES is currently considered the strongest encryption protocol.
WPA3	This is the next generation of Wi-Fi security. All WPA3-enabled devices use the latest security methods, disallow outdated legacy protocols, and require the use of Protected Management Frames (PMF).

Authenticating a Home User

Home routers typically have two choices for authentication: WPA and WPA2, with WPA 2 having two authentication methods.

- **Personal** – Intended for home or small office networks, users authenticate using a pre-shared key (PSK). Wireless clients authenticate with the wireless router using a pre-shared password. No special authentication server is required.
- **Enterprise** – Intended for enterprise networks. Requires a Remote Authentication Dial-In User Service (RADIUS) authentication server. The device must be authenticated by the RADIUS server and then users must authenticate using 802.1X standard, which uses the Extensible Authentication Protocol (EAP) for authentication.

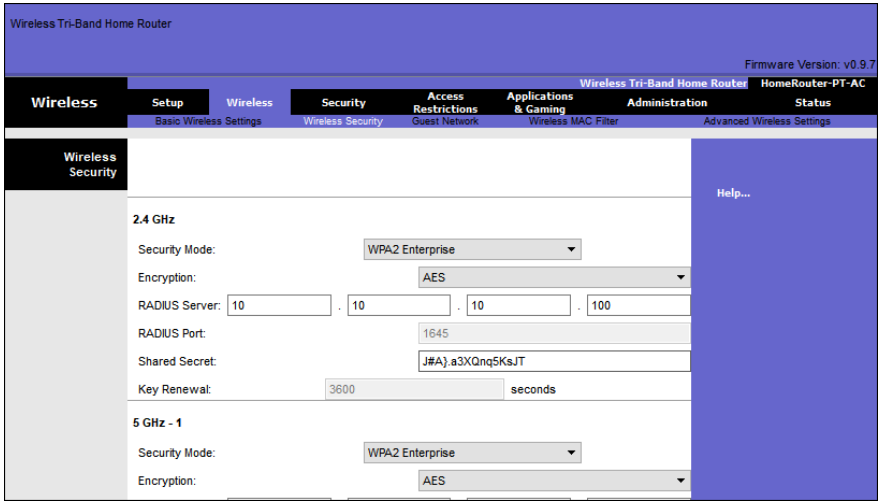


Authentication in the Enterprise

Enterprise security mode choice requires an Authentication, Authorization, and Accounting (AAA) RADIUS server.

There pieces of information are required:

- **RADIUS server IP address** – IP address of the server.
- **UDP port numbers** –UDP ports 1812 for RADIUS Authentication, and 1813 for RADIUS Accounting, but can also operate using UDP ports 1645 and 1646.
- **Shared key** – Used to authenticate the AP with the RADIUS server.



Note: User authentication and authorization is handled by the 802.1X standard, which provides a centralized, server-based authentication of end users.

WPA 3

Because WPA2 is no longer considered secure, WPA3 is recommended when available. WPA3 Includes four features:

- **WPA3 – Personal :** Thwarts brute force attacks by using Simultaneous Authentication of Equals (SAE).
- **WPA3 – Enterprise :** Uses 802.1X/EAP authentication. However, it requires the use of a 192-bit cryptographic suite and eliminates the mixing of security protocols for previous 802.11 standards.
- **Open Networks :** Does not use any authentication. However, uses Opportunistic Wireless Encryption (OWE) to encrypt all wireless traffic.
- **IoT Onboarding :** Uses Device Provisioning Protocol (DPP) to quickly onboard IoT devices.

12.8 Module Practice and Quiz